

# Transparent and Accountable Charity system using Block Chain Technology

S Ghousia Farheen Taj <sup>[1]</sup>, V.Mamatha <sup>[2]</sup>

Computer Science Department, VTU, Bengaluru

## ABSTRACT

Blockchain is a promising technology and is becoming predominant for solving many problems in the field related to security under the control of both public and private sectors. Blockchain is gaining popularity within the domain of charity. Due to lack of transparency in the transactions involved in Donations the donor(s) are not able to know whether their donations are being utilized properly, which has made people lose trust in Charities. The paper proposes a Blockchain based Decentralized Donation tracking system built on Hyperledger Blockchain which will provide full transparency, accountability and direct reach to the intended recipients. The current systems lack transparency in the field of Charity & Donations. In case of transactions associated with Donations made to different Organization(s) there's no proper maintenance of records and because of involvement of some corrupt peoples within the organization, has made people lose trust in this social cause. The donor is unaware whether their funds are being utilized properly or not. Corruption is the other reason that leads the donor to lose trust in charities.

**Keywords** — Blockchain, Decentralization, Chain Code, Hyper Ledger, Traceability, Consensus, Charity

## I. INTRODUCTION

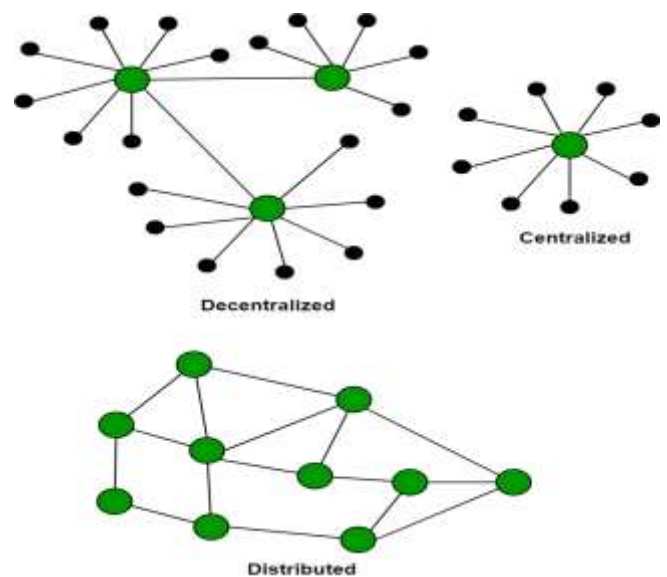
Blockchain is the backbone Technology of Digital Crypto Currency BitCoin. The blockchain is a distributed database of records of all transactions or digital event that have been executed and shared among participating parties. Each transaction verified by the majority of participants of the system. It contains every single record of each transaction. BitCoin is the most popular cryptocurrency an example of the blockchain. Blockchain Technology first came to light when a person or Group of individuals name 'Satoshi Nakamoto' published a white paper on "BitCoin: A peer to peer electronic cash system" in 2008. Blockchain Technology Records Transaction in Digital Ledger which is distributed over the Network thus making it incorruptible. Anything of value like Land Assets, Cars, etc. can be recorded on Blockchain as a Transaction.

Blockchain builds trust through the following five attributes:

- **Distributed:** The distributed ledger is shared and updated with every incoming transaction among the nodes connected to the Blockchain. All this is done in real-time as there is no central server controlling the data.
- **Secure:** There is no unauthorized access to Blockchain made possible through Permissions and Cryptography.
- **Transparent:** Because every node or participant in Blockchain has a copy of the Blockchain data, they have access to all transaction data. They themselves can verify the identities without the need for mediators.

- **Consensus-based:** All relevant network participants must agree that a transaction is valid. This is achieved through the use of consensus algorithms.

- **Flexible:** Smart Contracts which are executed based on certain conditions can be written into the platform. Blockchain Network can evolve in pace with business processes.



**Figure 1. Block Diagram**

Blockchain Network can evolve in pace with business processes. In a nutshell, here's how blockchain allows transactions to take place:

- A blockchain network makes use of public and private keys in order to form a digital signature ensuring security and consent.

Once the authentication is ensured through these keys, the need for authorization arises. Blockchain allows participants of the network to perform mathematical verification and reach a consensus to agree on any particular value.

- While making a transfer, the sender uses their private key and announces the transaction information over the network. A block is created containing information such as digital signature, timestamp, and the receiver’s public key.

- This block of information is broadcasted through the network and the validation process starts.

- Miners all over the network start solving the mathematical puzzle related to the transaction in order to process it. Solving this puzzle requires the miners to invest their computing power.

- Upon solving the puzzle first, the miner receives rewards in the form of bitcoins. Such kind of problems is referred to as proof-of-work mathematical problems.

- Once the majority of nodes in the network come to a consensus and agree to a common solution, the block is time stamped and added to the existing blockchain. This block can contain anything from money to data to messages.

- After the new block is added to the chain, the existing copies of blockchain are updated for all the nodes on the network.

## II. LITERATURE SURVEY

Hadi Saleh et al. [1] shows a method is to offer transparent accounting of operations donors, charitable foundations and recipients based on blockchain technology, charitable platform should provide transparent donation route, enable public users and donors to track and monitor where, when and to whom went resources of charity funds.

Aashutosh Singh et al. [2] proposed a propose a Blockchain based Decentralized Donation tracking system built on Ethereum Blockchain which willAn easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it provide full transparency, accountability and direct reach to the intended recipients.

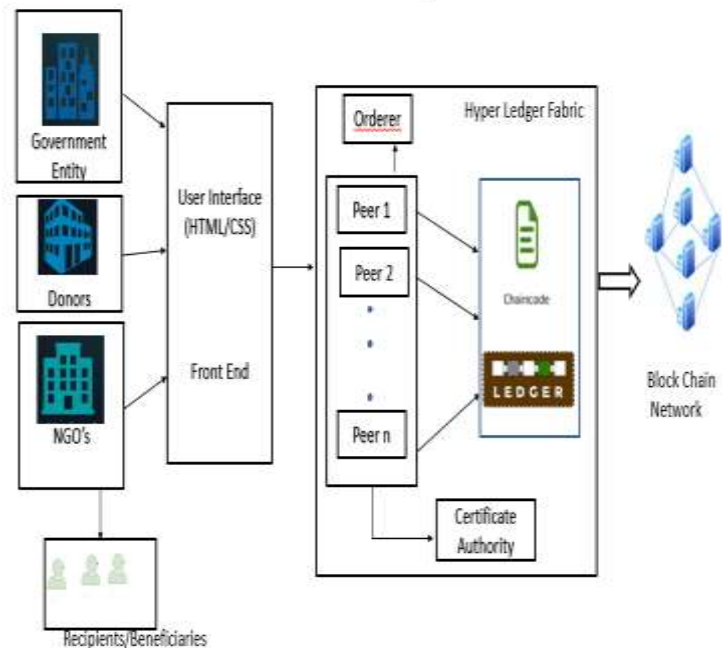
Dr.Chitra Kiran.N et al. [3] proposed an approach and module by which one payee module can communicate with the payer module using Bluetooth for money transfer from the payer’s to the payee’s bank. The significance of this approach is that it eliminates the physical need of case cash and serves for all types of payment and identity needs. The security of this module is intensified using biometric authentication.

Iyolita Islam et al. [4] proposed a to propose a money transfer system to automate and enhance the security of payment process for SMEs(Small and Medium Enterprises) in Bangladesh. The proposed system includes iris verification technique to authenticate a user uniquely and consistently over the time.

Reza Mauliadi et al. [5] presented a survey platform to generate the charities systems with ABS(Abstract Behavioral Specification) as a core architecture to support SPL(Software Product Lines). They endeavour to develop an adaptive system for different charity organizations in a single development with Software Product Lines (SPL) as its approach to deal with the charities problems.

Rajesh Kannan Megalingam et al. [6] presented a survey which the design of an intelligent donation box, capacitated to request for charity. This scheme is anticipated to be even more effective than merely placing a donation box in a conspicuous location or a human directly asking for charity. This can be used to raise funds for the welfare of the needy.

## III. SYSTEM ARCHITECTURE



**Figure 2. Block Diagram of Charity System using Block chain**

The block diagram is represented in figure 1 .It shows that there are 3 different types of users like NGO, GOVT, DONOR. First, NGO (Non- Government Organization) will register into the Block chain network by giving his details like Name, Contact No, Description of his Organization, Organization Name, Cause of Donation, Address. After submitting his details his account will be successfully created in the Block chain network. Now, GOVT is the entity who acts like admin, he can approve the request or reject his request based upon some unique and genuine identity. After approving only the NGO’s request will be visible to Donor. Donor should also register in the network if he is coming for the first time. After successful registration by providing details like Name, Address, Contact number, Account details, etc. Donor can choose his own NGO and can transfer the

money. The transaction of money will be stored in the distributed ledger of the Block chain where all the other users are registered, Even GOVT entity can track the NGO’s actions and the Donor’s actions.

#### IV. IMPLEMENTATION & METHODOLOGY

##### Hyperledger Fabric:

Hyperledger Fabric is a blockchain platform for distributed ledger solutions underpinned by a modular architecture delivering high degrees of confidentiality, resiliency, flexibility, and scalability. It is designed to support pluggable implementations of different components and accommodate the complexity and intricacies that exists across the economic ecosystem.

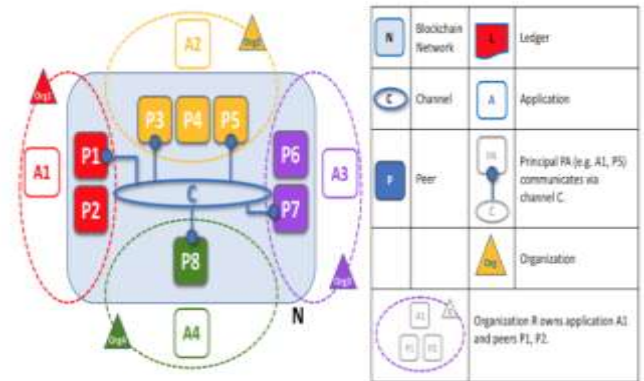


Figure 3. Block Diagram of Hyperledger Fabric

##### Components of Hyperledger Fabric Network:

- Ledger** : A ledger consists of two distinct, though related, parts — a “blockchain” and the “state database”, also known as “world state”. Unlike other ledgers, blockchains are immutable — that is, once a block has been added to the chain, it cannot be changed.
- Membership Service Provider** : The Membership Service Provider (MSP) refers to an abstract component of the system that provides credentials to clients, and peers for them to participate in a Hyperledger Fabric network.
- Smart Contract** : A smart contract is code — invoked by a client application external to the blockchain network — that manages access and modifications to a set of key-value pairs in the World State.
- Peers** : A network entity that maintains a ledger and runs chaincode containers in order to perform read/write operations to the ledger. Peers are owned and maintained by members.
- Ordering Service** : A defined collective of nodes that orders transactions into a block. The ordering service exists independent of the peer processes and orders transactions on a first-come-first-serve basis for all channel’s on the network.
- Channel** : A channel is a private blockchain overlay which allows for data isolation and confidentiality. A channel-specific ledger is shared across the peers in the channel, and transacting parties must be properly authenticated to a channel in order to interact with it.
- Certificate Authority** : Hyperledger Fabric CA is the default Certificate Authority component, which issues PKI-based certificates to network member organizations and their users.
- Organizations** : Also known as “members”, organizations are invited to join the blockchain network by a blockchain service provider. An organization is joined to a network by adding its Membership Service Provider to the network.

The following are prerequisites for installing the required development tools:

- Operating Systems: Ubuntu Linux 14.04 / 16.04 LTS (both 64-bit), or Mac OS 10.12
- Docker Engine: Version 17.03 or higher
- Docker-Compose: Version 1.8 or higher
- Node: 8.9 or higher (Note: version 9 is not supported)
- npm: v5.x
- git: 2.9.x or higher
- Python: 2.7.x
- VSCode.

##### Steps of Starting Hyperledger Fabric

1. Open docker-compose-base.yaml file which is present in the bin folder and introduce following changes.

Change orderer volume binding to ../composer-genesis.block:/var/hyperledger/orderer/orderer.genesis.block

Change peer volume binding to (for all 4 peers)-  
- ../etc/configtx

2. To start fabric, run the following command –

```
docker-compose -f docker-compose-cli.yaml -f docker-compose-couch.yaml up -d 2>&1
```

3. After completing all these steps , you can run command -

```
docker ps -a
```

This will list all running containers regarding our network setup, in our case it will list 10 containers.

```

CONTAINER ID        IMAGE               COMMAND             CREATED             STATUS
PORTS
baff6e9a892       hyperledger/fabric-peer:latest    "peer node start"  4 hours ago        Up 3 hours
peer1.org1.example.com
5d69fab45269       hyperledger/fabric-peer:latest    "peer node start"  4 hours ago        Up 3 hours
peer8.org2.example.com
ee4b381b7686       hyperledger/fabric-peer:latest    "peer node start"  4 hours ago        Up 3 hours
peer8.org1.example.com
5178f9426a22       hyperledger/fabric-peer:latest    "peer node start"  4 hours ago        Up 3 hours
peer1.org2.example.com
ec8f9ef17239       hyperledger/fabric-couchdb        "tini -- /docker-ent..."  4 hours ago        Up 4 hours
4369/tcp, 9106/tcp, 8.9.8.0:8984->9106/tcp couchdb3
2b46e94efcfe       hyperledger/fabric-couchdb        "tini -- /docker-ent..."  4 hours ago        Up 4 hours
4369/tcp, 9106/tcp, 8.9.8.0:7984->9106/tcp couchdb2
7922825a627e       hyperledger/fabric-couchdb        "tini -- /docker-ent..."  4 hours ago        Up 4 hours
4369/tcp, 9106/tcp, 8.9.8.0:5984->9106/tcp couchdb0
6d779e1740e       hyperledger/fabric-couchdb        "tini -- /docker-ent..."  4 hours ago        Up 4 hours
4369/tcp, 9106/tcp, 8.9.8.0:6984->9106/tcp couchdb1
18838d1ccf5e       hyperledger/fabric-tools:latest    "/bin/bash"        11 hours ago       Up 11 hours
cli
chef3866c85       hyperledger/fabric-orderer:latest  "orderer"          11 hours ago       Up 11 hours
8.0.0.8:7050->7050/tcp orderer.example.com
    
```

Figure 4. Output of the above command in the terminal



Figure 6. Sign up page

Proposed network setup is complete, our network have -

- One orderer
- Two Organizations
- Four peers (two peers on each organization)
- Couchdb for all peers

4. Creating channel
5. Joining first peer where channel is created
6. Install chainCode on every machine
7. Start chaincode on one machine

In the Login module, there are 3 different users NGO, Donor, GOVT. All 3 users have their own Sign up and sign pages.



Figure 6. Sign in page

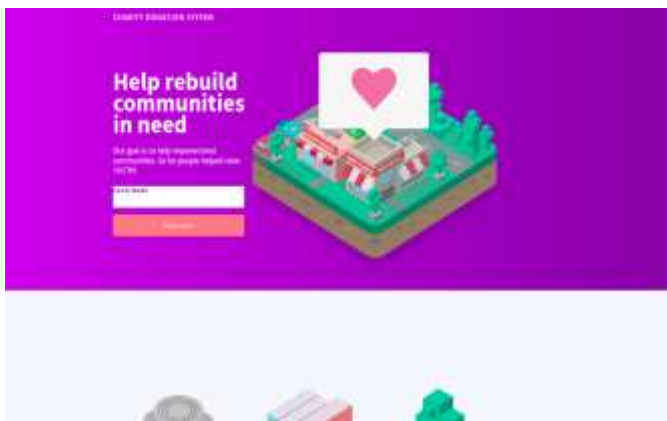


Figure 5. Home page

Sign up and Sign in page will be present for each user.

Each user should be able to create his own account which will be stored in the distributed ledger of the Block chain network. They have to input certain fields like Name, Address, Contact Number, Aadhar number, Account details, Organization name, description of the organization etc.

After Successful registration in the network, the user details are stored in the Couchdb database. In which all the information is stored in the Key value pair and in the encrypted format.

Name	Size	# of Docs	Actions
replicator	2.8 KB	1	⌵ ⌵ ⌵
users	2.8 KB	1	⌵ ⌵ ⌵
mychannel	13.8 KB	2	⌵ ⌵ ⌵
mychannel_led	12.8 KB	2	⌵ ⌵ ⌵
mychannel_malike	1.3 KB	3	⌵ ⌵ ⌵
mychannel_myc	1.8 KB	2	⌵ ⌵ ⌵

Figure 7. Couchdb page



## V. CONCLUSIONS

The focus of this paper is to compare the different methods for donating or transferring the money from one person to another person. From the above comparisons we can conclude that the Decentralized Donation Tracking System based on Smart Contract on blockchain technology helps record the transactions of individual(s) making donations and gather information of where the donations are being spent. Smart contracts using blockchain implemented helps in controlling the transfer of tokens or digital currencies between the ends parties involved in the transaction directly without the need to depend on a trusted third party.

## REFERENCES

1. "Platform for Tracking Donations of Charitable Foundations based on Blockchain Technology", Hadi Saleh, Sergey Avdoshin, ©2017 IEEE.
2. "Aid, Charity and Donation Tracking System Using Blockchain", Aashutosh Singh, Rohan Rajak, ©IEEE 2020
3. "A Biometric based Payment System by using Payee and Payer Module", Dr. Chitra Kiran.N, Suchira Suresh, ©2017 IEEE.
4. "A Proposed Secure Mobile Money Transfer System for SME in Bangladesh: An Industry 4.0 Perspective", Iyolita Islam, Kazi Md. Munim, ©2019 IEEE.
5. "A Platform for Charities System Generation with SPL Approach", Reza Mauliadi, Maya R. A. Setyautami, © IEEE 2017
6. "Voice Enabled Donation Box", Rajesh Kannan Megalingam1, Balla Tanmayi, © IEEE 2019
7. "Credit Card Fraud Detection on the Skewed Data Using Various Classification and Ensemble Techniques", Ankit Mishra, Chaitanya Ghorpade, © IEEE 2018
8. "Achieving Privacy and Security using QR Code by means of Encryption Technique in ATM", Malathi V, Balamurugan B, © IEEE 2017
9. "Instant Secure Mobile Payment Scheme", Mahmoud Obaid 1, Zeki Bayram 1, Murad Saleh, © IEEE 2018
10. "SDD Sentinel: a Support Tool for Detecting and Investigating Electronic Transaction Frauds", Gaetano Papale, Luigi Sgaglione, © IEEE 2017
11. "Review On Fraud Detection Methods in Credit Card Transactions", Krishna Modi, Reshma Dayma, © IEEE 2017
12. "Designing a Smart Mobile Application to Detect Fraud Theft of E-Banking Access Based on SOA In Indonesia", Meyliana, Ahmad Nurul Fajar, © IEEE 2019
13. "Secure and Energy Efficient Mobile Payment Protocol", Abdul Razaque, Fathi Amsaad, © IEEE 2018
14. "Application of Blockchain Technology based Credit System for Personal Financial information", Zhiyuan Chang, © IEEE 2020
15. "Future Generation Computer Systems", Ahmed Khan, Khaled salah, © Elsevier 2018
16. "A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography", Shehzad Ashraf Chaudhry, © Springer 2016
17. "Mobile Payment Security, Threats, and Challenges", Yong Wang, Christen Hahn, © IEEE 2016
18. "Information Security in Virtualized Data Center Network", Mykhailo Klymash, Olga Shpur, © IEEE 2019
19. "Data Security issues in Cloud", Lalitha V.P, © IEEE 2017.
20. "Emergence and Growth of Mobile Money in Modern India: A Study on the Effect of Mobile Money", Mukund Jakhiya, Dr. Harsh Purohit, © 2020 IEEE